IBM System z9 and zSeries

IT Sicherheit mit z/VSE

Ingo Franzki

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and / or other counties.

CICS*
DB2*
DB2 Connect
DB2 Universal Database
e-business logo*
Enterprise Storage Server
HiperSockets
IBM*
IBM logo*
IMS
Intelligent Miner
Multiprise*
MQSeries*
OS/390*
S/390*
SNAP/SHOT*
Virtual Image Facility
VM/ESA*
VSE/ESA
VisualAge*
VTAM*
WebSphere*
xSeries
z/Architecture
z/VM
z/VSE
zSeries

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

LINUX is a registered trademark of Linus Torvalds

Tivoli is a trademark of Tivoli Systems Inc.

Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries

UNIX is a registered trademark of The Open Group in the United States and other countries.

Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.

SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.

Intel is a registered trademark of Intel Corporation.

IT Sicherheit im Unternehmen

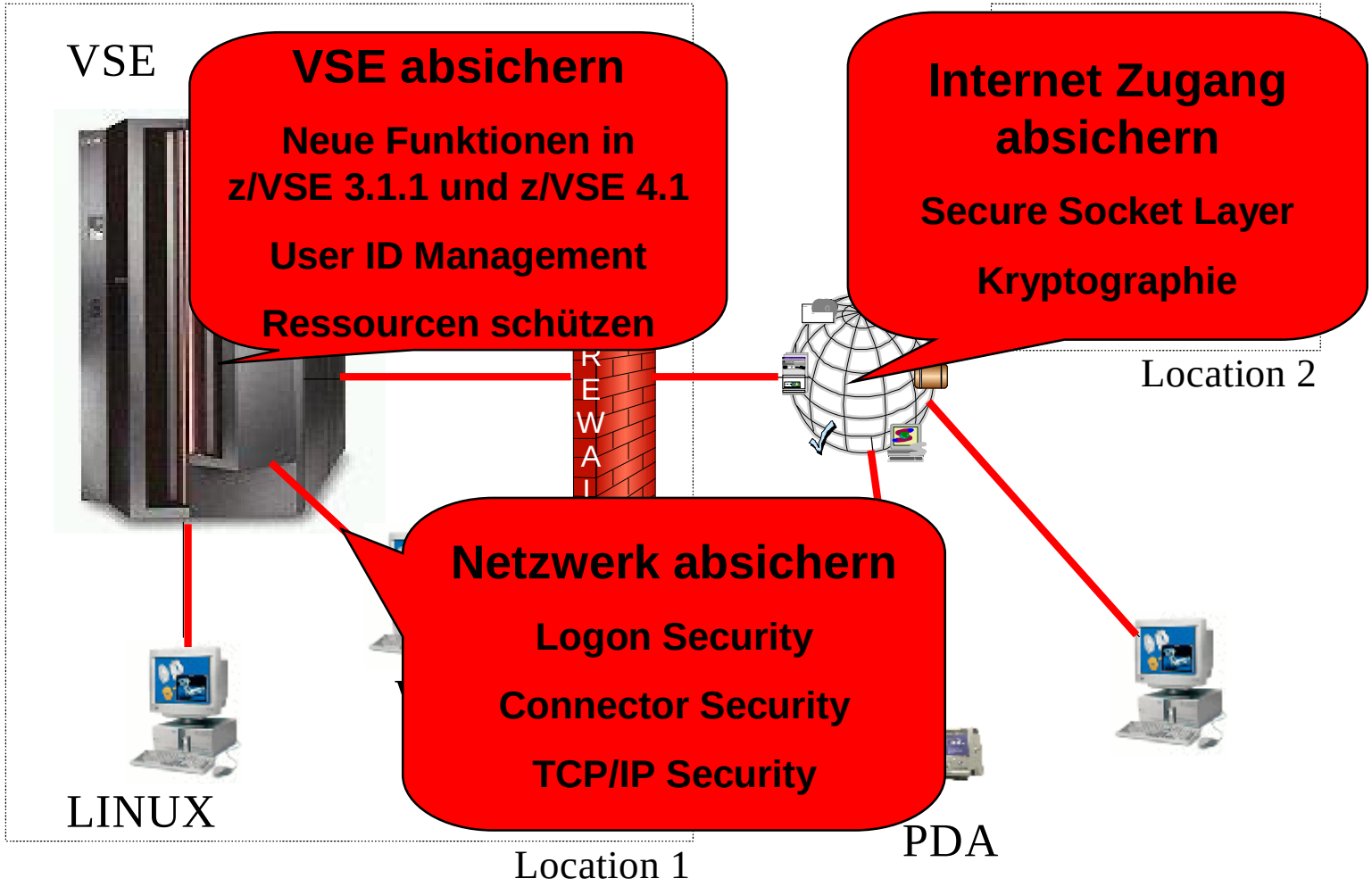
- **Die Anforderungen an den Datenschutz steigen ständig**
  - Datensicherheit
  - Datenintegrität
  - Audit-sicheres Speichern von Daten
- **Die Attacken auf IT Systeme werden ständig mehr**
  - Industrie-Spionage
  - Einbruchsversuche, Denial-of-Servcie Angriffe
  - Spam, Phishing, …
- **Nichtbeachtung von Security-Anforderungen kann sehr teuer werden**
  - Die Daten Ihres Unternehmens sind Ihre „(Über-) Lebensversicherung“
  - Schadensersatz-Forderungen bei Verlust von Kunden-Daten
  - Imageverlust kostet Kunden
- **IT Sicherheit wird immer wichtiger**
  - Es muss die gesamte IT-Landschaft betrachtet werden, nicht nur einzelne Systeme

IT Sicherheit im Unternehmen - Haftung

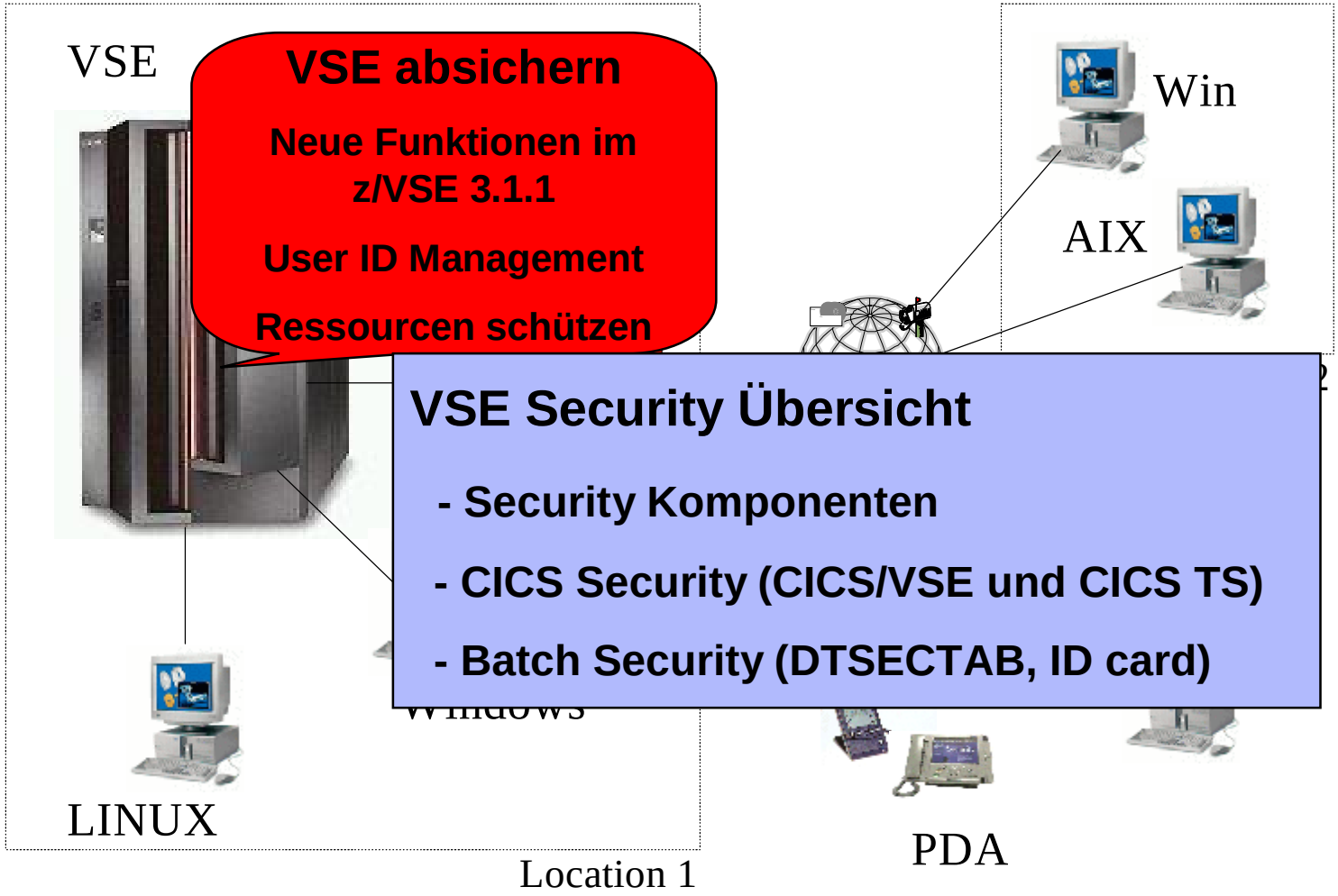
- **Firmenchefs haften für Sicherheit**
  - Wenn durch schlecht geschützte IT-Systeme Schaden entsteht, müssen die Verantwortlichen unter Umständen persönlich dafür aufkommen.
- **Das Thema IT-Sicherheit hat längst nicht mehr nur technische Aspekte**
  - Die gesetzlichen Vorschriften sollten besonders bei geschäftsverantwortlichen Firmenlenkern ganz oben auf der Agenda stehen
  - Für eventuelle Folgeschäden von Sicherheitslücken könnten sie persönlich in die Pflicht genommen werden.
- **Das KonTraG nimmt den Vorstand in die Pflicht**
  - Seit dem 1998 verabschiedeten Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) enthält auch das Aktiengesetz (Paragraf 91 II AktG) eine Regelung, nach der der Vorstand geeignete Maßnahmen zu treffen und ein Überwachungssystem einzurichten hat, so dass er "den Fortbestand der Gesellschaft gefährdende Entwicklungen" frühzeitig erkennen kann.
  - Das setzt ein effizientes Risiko-Management voraus.
  - Im IT-Bereich sind ein ausreichender Schutz der IT-Infrastruktur - durch Datensicherung - sowie Präventivmaßnahmen gegen Angriffe von außen und missbräuchliche Nutzung durch Mitarbeiter notwendig.

Quelle: Computerwoche 38/2006
http://www.computerwoche.de/heftarchiv/2006/38/1216038/index.html

IT Sicherheit in einem heterogenen Umfeld



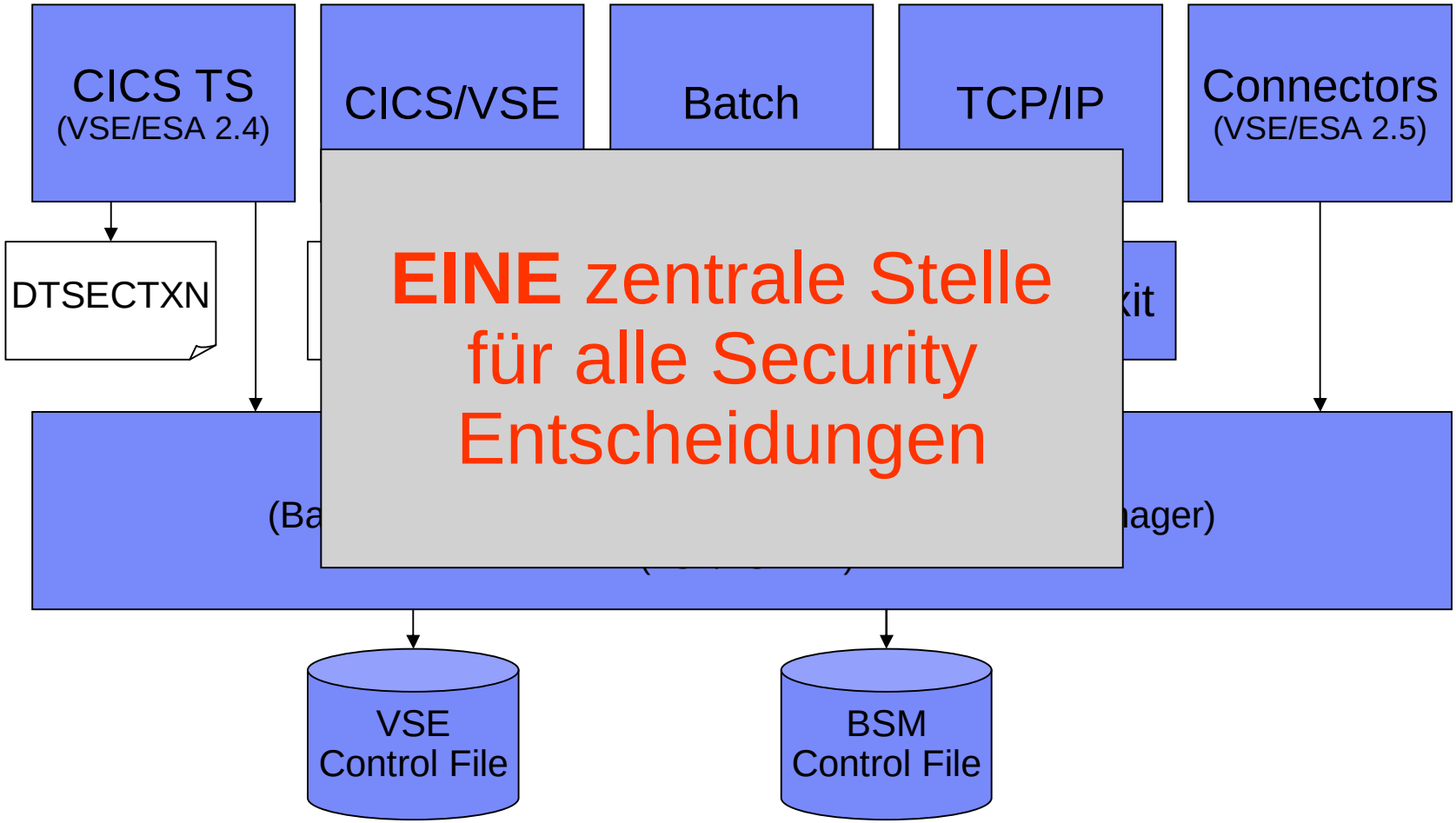
IT Sicherheit in einem heterogenen Umfeld



Warum überhaupt VSE absichern?

- **Unerlaubten Zugriff auf VSE und Daten verhindern**
  - Um die Daten geheim zu halten
    - Kundedaten, Datenschutz, Industrie-Spionage
  - Datenmodifikation verhindern (gewollt/ungewollt)
    - Unternehmenskritische Daten
- **Benutzer davon abhalten das VSE System zu beschädigen**
  - Unbeabsichtigtes Löschen/Verändern von Daten
    - Audit-Sicheres Speichern der Daten
  - Datenintegrität sicher stellen
- **Ihre Produktionsdaten sind Ihr Kapital**
  - Die Produktionsdaten unterscheiden Sie von Ihren Konkurrenten

Security Komponenten im VSE



Basic Security Manager – Neu mit z/VSE 3.1.1

- **Benutzer können in Gruppen kategorisiert werden**
  - Vereinfacht das User-ID Management
  - Berechtigungen können basierend auf der Gruppenzugehörigkeit vergeben werden
- **„Description“ Feld für alle Profile (20 Zeichen)**
  - Einfachere Zuordnung zu realen Personen, Ressourcen
- **Neue Administrationsfunktionen**
  - BSTADMIN (Konsole oder Batch)
  - Interactive Interface Dialogs
- **Neue Ressource Klassen**
  - TCICSTRN - Transaktionen
  - MCICSPPT - Anwendungs-Programme
  - FCICSFCT - Dateien
  - JCICSJCT - Journale
  - SCICSTST - Temporary Storage Queues
  - DCICISDCT - Transient Data Queues
  - ACICSPCT - Transaktionen (CICS START)
  - APPL - Anwendungen
  - FACILITY - Spezielle Ressourcen

Basic Security Manager – Neu mit z/VSE 4.1

- **Audit-Logging und Reporting**
  - Alle Zugriffe auf geschützte Ressourcen können protokolliert werden
    - Sowohl erlaubte als auch unerlaubte Zugriffe
  - Versuchte Angriffe können erkannt werden
    - z.B. mehrfache Logon-Versuche mit falschem Passwort
  - Man kann nachvollziehen wer wann welche Ressource im Zugriff hatte
  - Auswertung mit Hilfe eines Report-Tools
    - Zusammenfassung
    - Detaillierte Auflistung aller Zugriffe
  - Benützt das CICS DMF Tool
    - Erstellt SMF Records für Protokol-Informationen

CICS Security

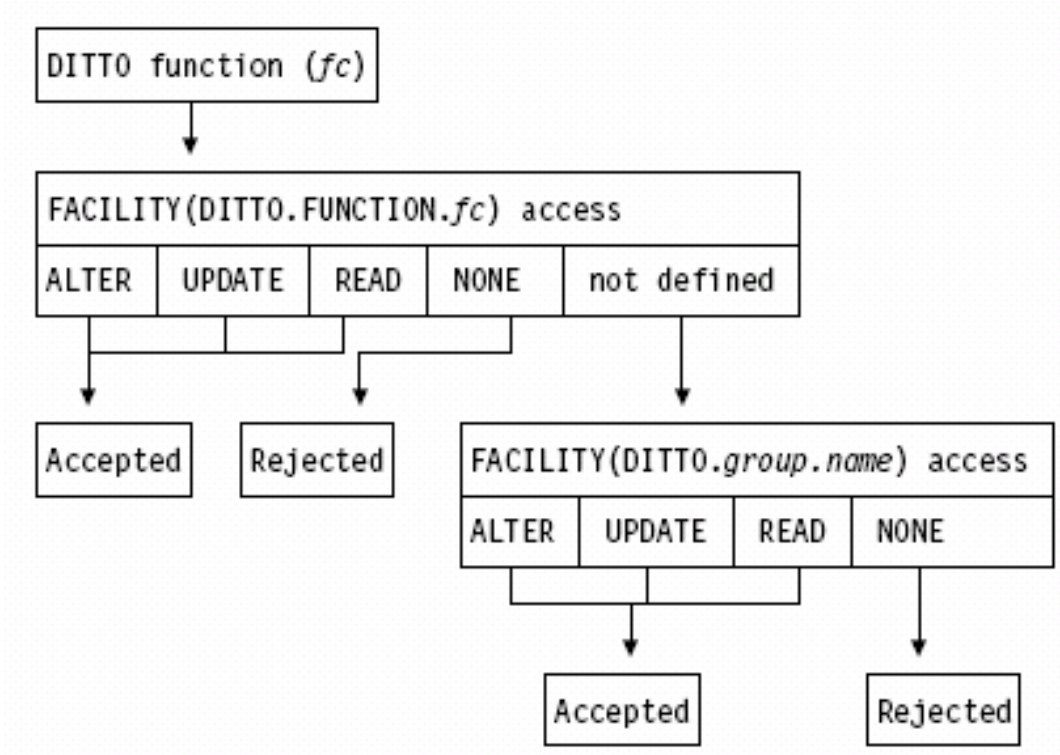
- **Logon Security**
  - Logon nur für berechtigte Personen möglich
  - Berechtigungen für Anwendungen und Ressourcen des Benutzers
- **Resource Security**
  - CICS Ressourcen (z.B. Dateien, Anwendungen, …) können vor unerlaubtem Zugriff geschützt werden
  - Zugriffsrechte können sehr granular vergeben werden
- **Beispiel: Definition einer Datei (z.B. Datei FILEA und FILEB)**
  - DEFINE FILE: RESSEC(YES)
  - Mit BSTADMIN: Ressource Klasse FCICSFCT:
    - ADD FCICSFCT FILEA UACC(NONE)
    - ADD FCICSFCT FILEA UACC(NONE)
    - PERMIT FCICSFCT FILEA(GROUP1) ACCESS(UPDATE)
    - PERMIT FCICSFCT FILEB(GROUP1) ACCESS(READ)

Batch Security

- **Nur berechtigte Personen dürfen Jobs ausführen**
- **Jobs laufen unter der spezifizierten User ID**
  - Schützt vor unerlaubtem Zugriff und/oder Modifikation von Daten
  - Der Job hat die Berechtigungen des Benutzers unter dem er läuft
- **ID Statement oder * $$ JOB spezifiziert die User ID und Passwort für den Job**
  - Subsysteme (LIBR, VSAM, ...) benutzen diese User ID um Zugriffsberechtigungen zu prüfen
  - Erfordert SYS SEC=YES in der IPL Procedure

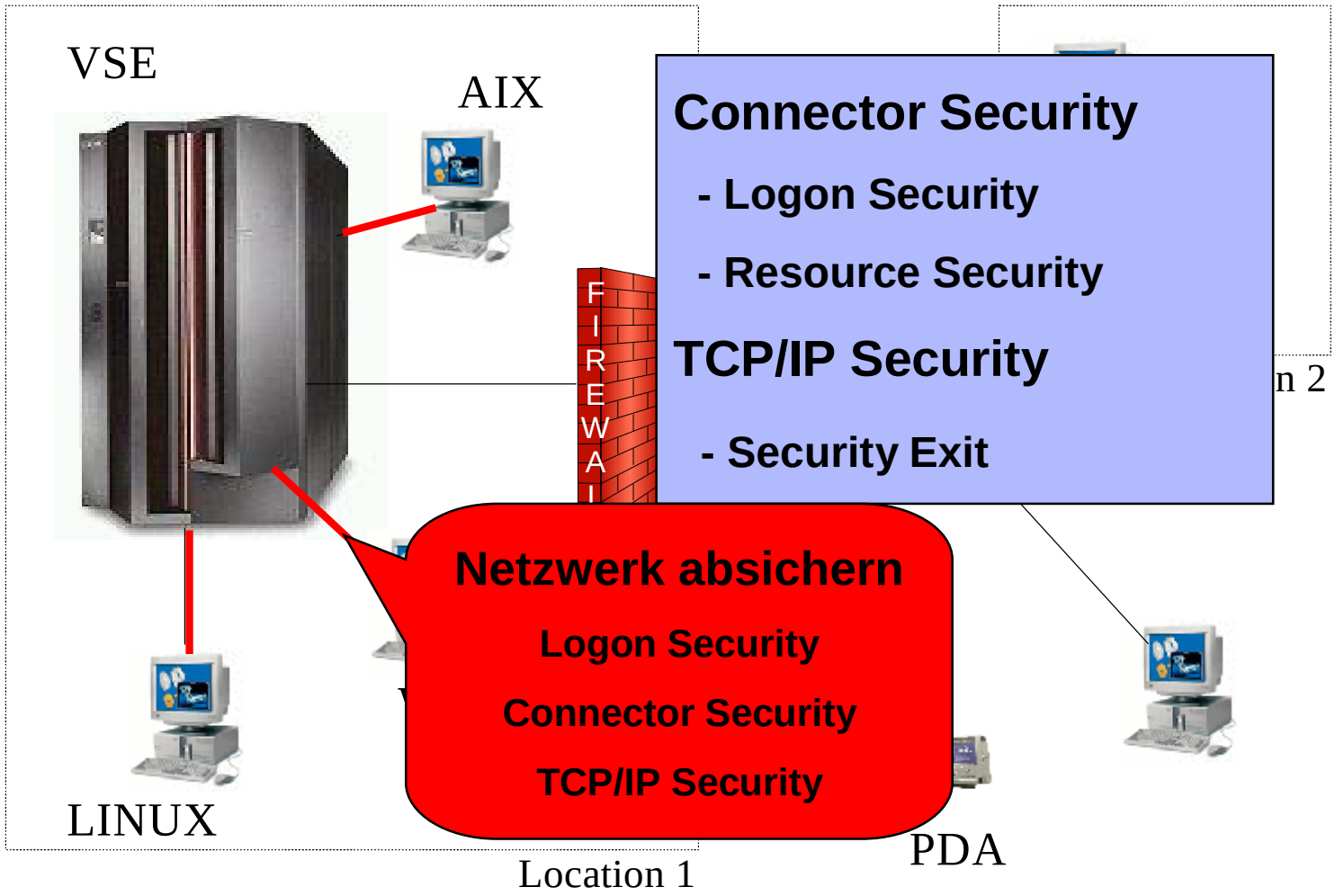
DITTO Security

- **DITTO verwendet FACILITY Profile um Zugriffe auf Daten zu schützen**



- **Batch Security muss aktiv sein**
  - IPL SEC=YES
- **FACILITY Profile müssen definiert sein**
- **ALTER, UPDATE oder/und READ bedeuten „erlaubt“ , nichts definiert bedeutet „Zugriff verweigert“**

IT Sicherheit in einem heterogenen Umfeld



Warum überhaupt das Netzwerk absichern ?

- **Heutzutage sind die meisten Rechner Teil eines Netzwerks**
  - Verteilte Prozesse erfordern Austausch von Daten zwischen den Systemen
  - Der Datenaustausch muss sicher und zuverlässig sein
  - Andere Systeme greifen auch auf VSE Anwendungen und Daten zu
  - Auch in einem vermeintlich sicheren Unternehmensinternen Netzwerk grassieren Viren und Würmer
  - Die gefährlichsten Angriffe sind die von Innen (frustrierte Mitarbeiter)
- **Unerlaubter Zugriff auf VSE und Daten muss verhindert werden**
  - Sichere Anmeldung am System muss gewährleistet sein
  - Abhörsichere Verbindung für Unternehmenskritische Daten
- **Mit FTP kann man theoretisch auf Produktions-Daten zugreifen**
  - z.B. VSAM, POWER Listen

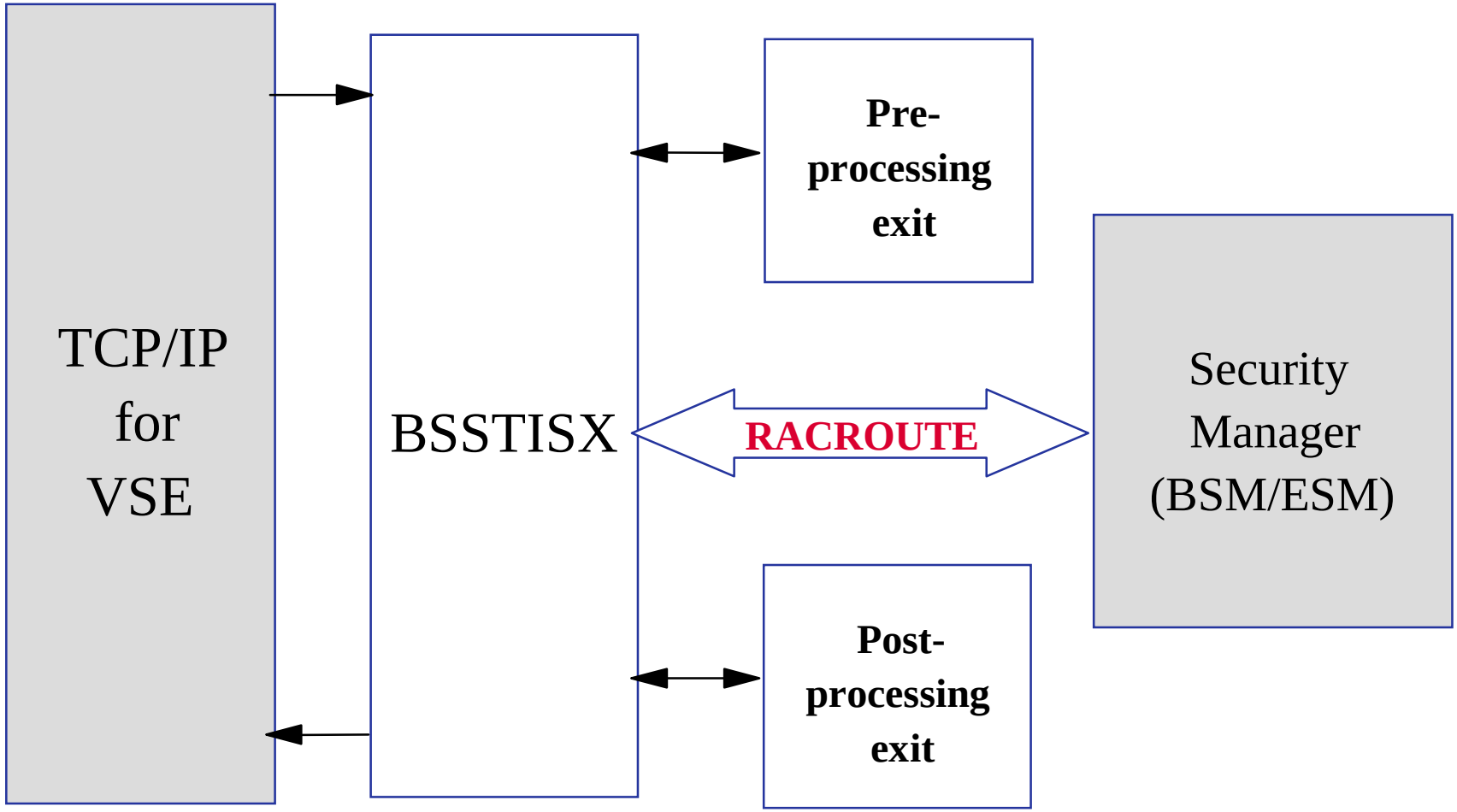
Connector Security

- **VSE Connector Server ist ein Ressource Manager (wie CICS)**
  - Benutzer müssen sich anmelden bevor sie Zugriff auf VSE Ressourcen haben
  - Jeder Ressource-Zugriff wird geprüft
    - Berechtigungen sind abhängig vom jeweiligen Benutzer
- **Kein zusätzliches User Profile Setup erforderlich**
- **Aber:**
  - Es ist möglich zusätzliche Restriktionen per User ID und/oder IP Adresse zu definieren
  - Neu mit z/VSE 4.1: Mittels FACILITY Profilen kann der Zugriff auf Subsystem-Level (z.B. LIBR, VSAM, …) gesperrt werden

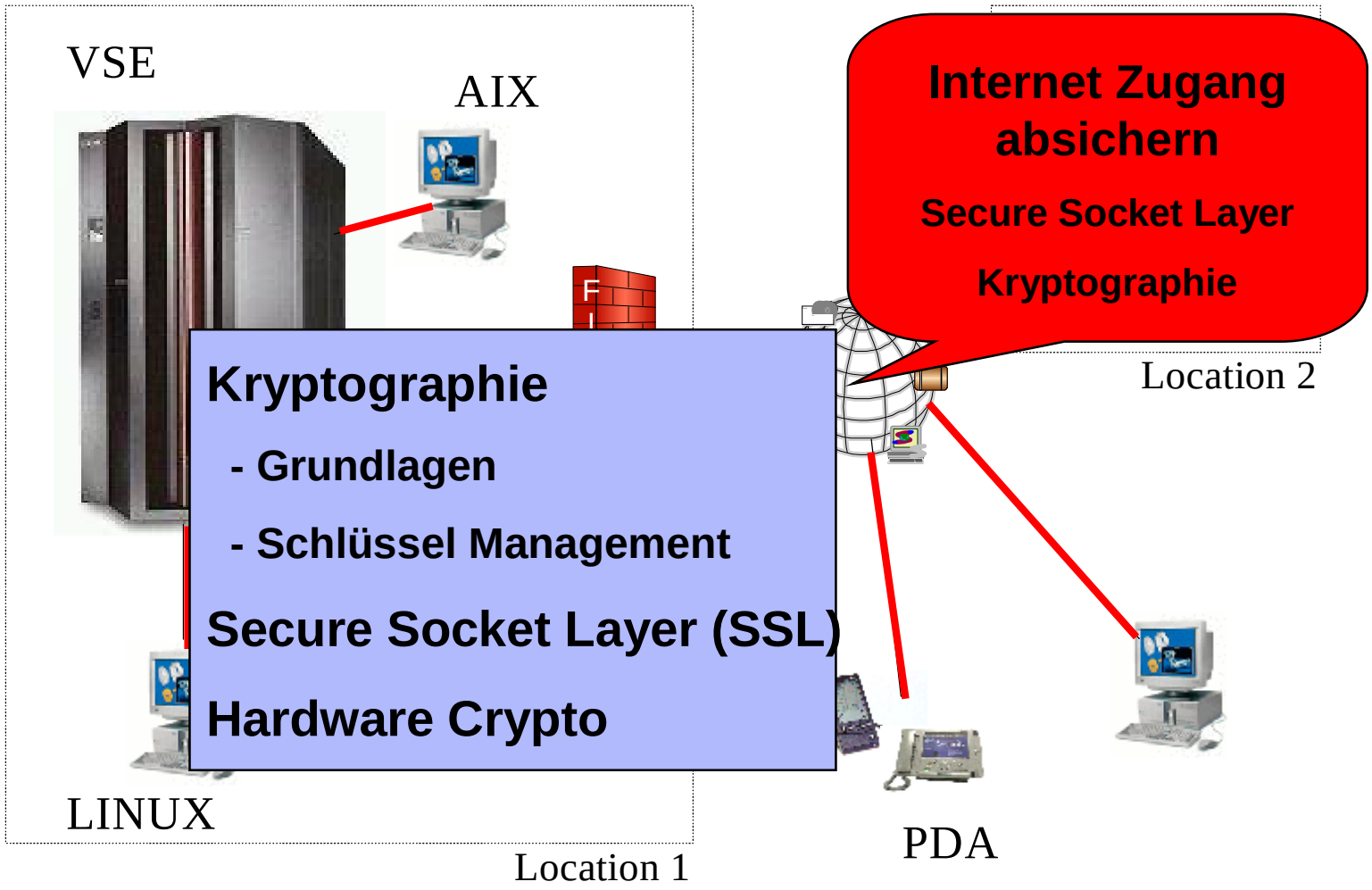
TCP/IP Security

- **Standardmäßig verwendet TCP/IP seine eigenen User IDs**
  - DEFINE USER,ID=user,PASSWORD=pwd
  - Im Klartext lesbar im Konfigurations-Member (IPINITxx.L)
  - Doppelte User Profile Definitionen
- **Security Exit von IBM**
  - Prüft User IDs bei Logon
  - Prüft Ressource-Zugriffe
- **Die meisten Angriffsversuche kommen über TCP/IP**
  - Hier ist Security besonders wichtig !

TCP/IP Security Exit



IT Sicherheit in einem heterogenen Umfeld



Anforderungen bezüglich Datenschutz

- **Die Anforderungen an den Datenschutz steigen ständig**
  - Datensicherheit
  - Datenintegrität
  - Audit-sicheres Speichern von Daten
- **Speziell beim Transport der Daten muss sichergestellt werden dass die Daten nicht verloren gehen oder kopiert werden können**

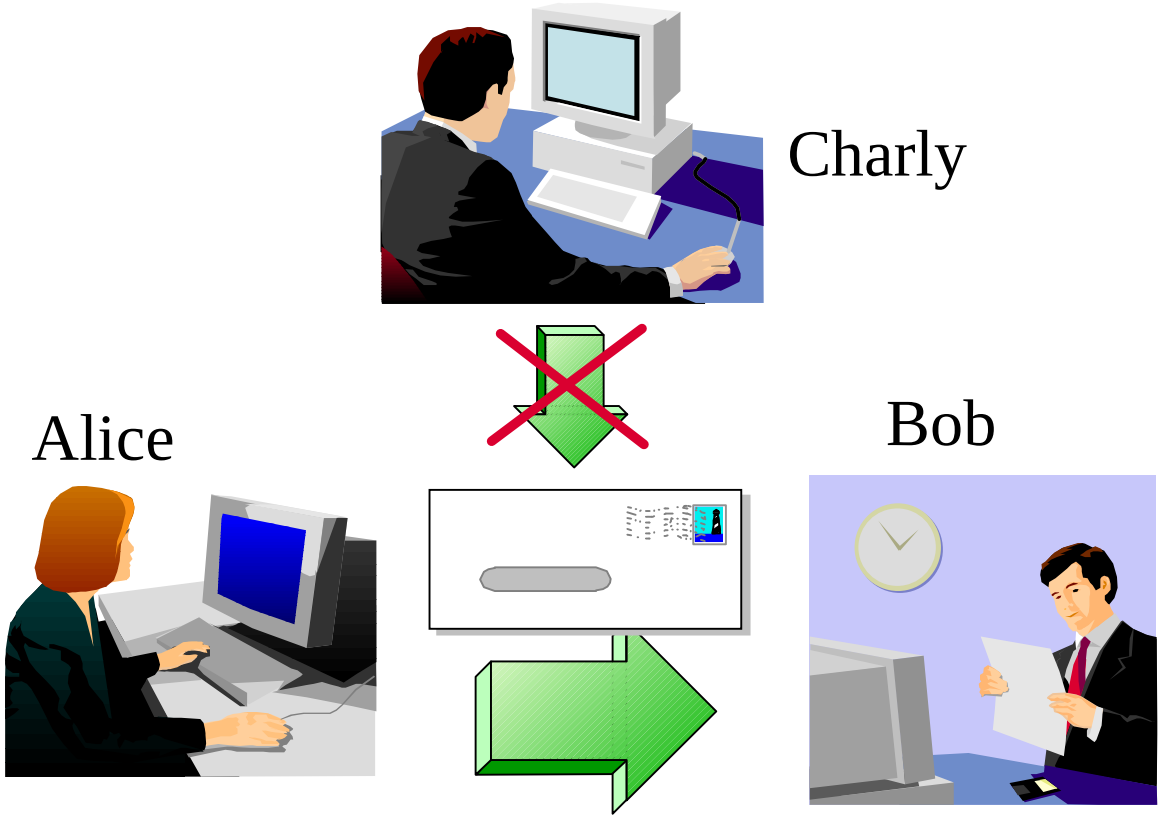
Zweigstelle

Business Partners

Warum überhaupt Kryptographie ?

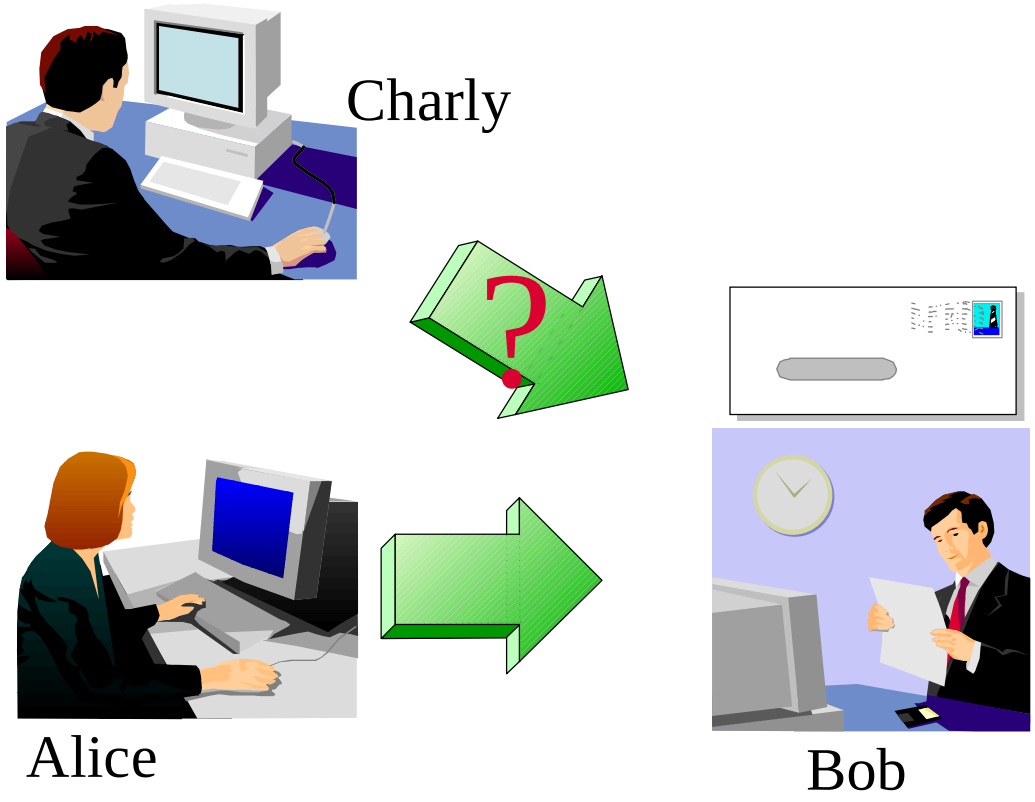
- **Um vertrauliche Daten geheim zu halten**
  - Kommunikation mit Partnern darf nicht abhörbar sein
  - Vertrauliche (interne) Daten dürfen nicht an Dritte gelangen
- **Identitäten von Benutzern prüfen**
  - Zugriff auf IT-Systeme nur durch autorisierte Personen
  - Nur ein eingeschränkter Personenkreis darf Zugriff haben auf Unternehmenskritische Daten
  - Ursprung von Informationen verifizieren (Spam, Phishing)
- **Unveränderbarkeit von Informationen sicherstellen**
  - Audit-sicheres Speichern oder Archivieren von Daten
  - Unveränderbarkeit der Daten sicherstellen bei elektronischer Kommunikation (z.B. e-Mail)

Vertrauliche Daten geheim zu halten



Alice verschlüsselt die Nachricht mit einem geheimen Schlüssel den nur sie und Bob kennnen

Identitäten von Benutzern prüfen



Alice "signiert" die Nachricht indem sie eine geheime Phrase anhängt, die nur sie und Bob kennen

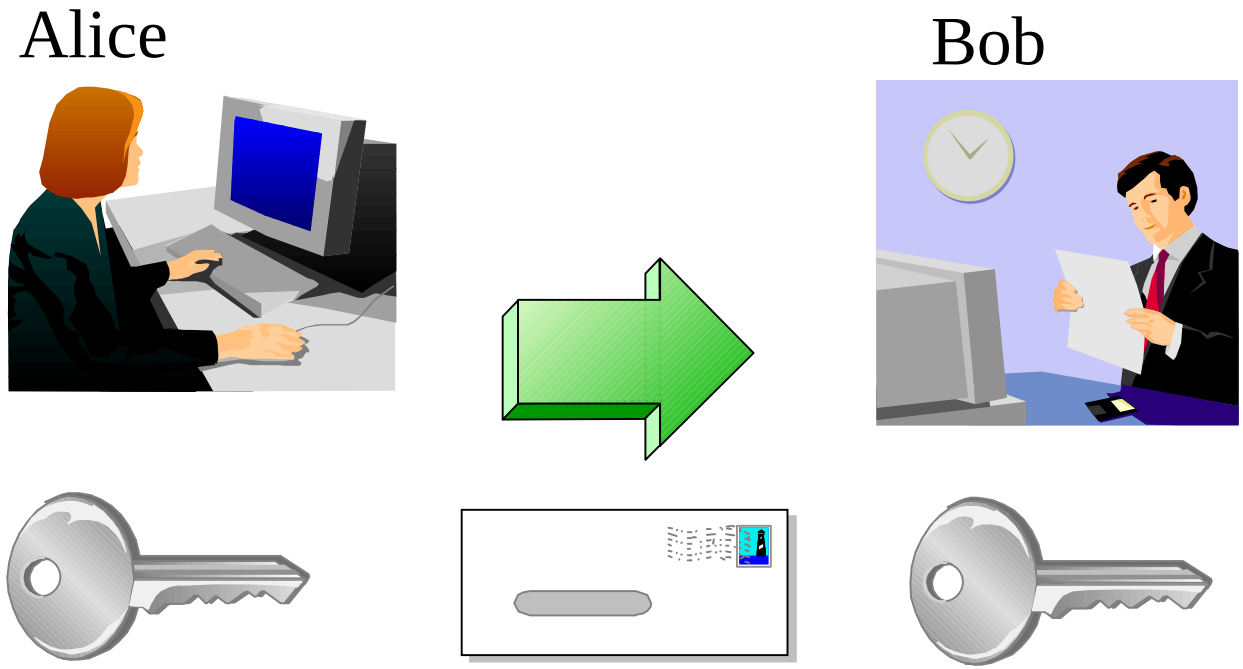
Unveränderbarkeit von Informationen sicherstellen

Alice generiert einen "Hash" aus der Nachricht mittels eines geheimen Schlüssels und hängt ihn an die Nachricht an. Bob generiert ebenfals einen Hash mit der empfangenen Nachricht und vergleicht ihn mit dem Hash von Alice.

Secret Key Kryptographie (symmetrisch)

- **Beide Partien kennen den selben geheimen Schlüssel**
- **Der Schlüssel muss geheim gehalten werden**
- **Verschlüsselungs-Algorithmus = mathematische Transformation der Daten mit dem Schlüssel**
  - DES Data Encryption standard
  - 3DES Triple strength DES
  - AES Advanced Encryption Standard
- **Typische Schlüssellängen: 40, 56, 128 oder 256 Bit**

Secret Key Kryptographie (symmetrisch)

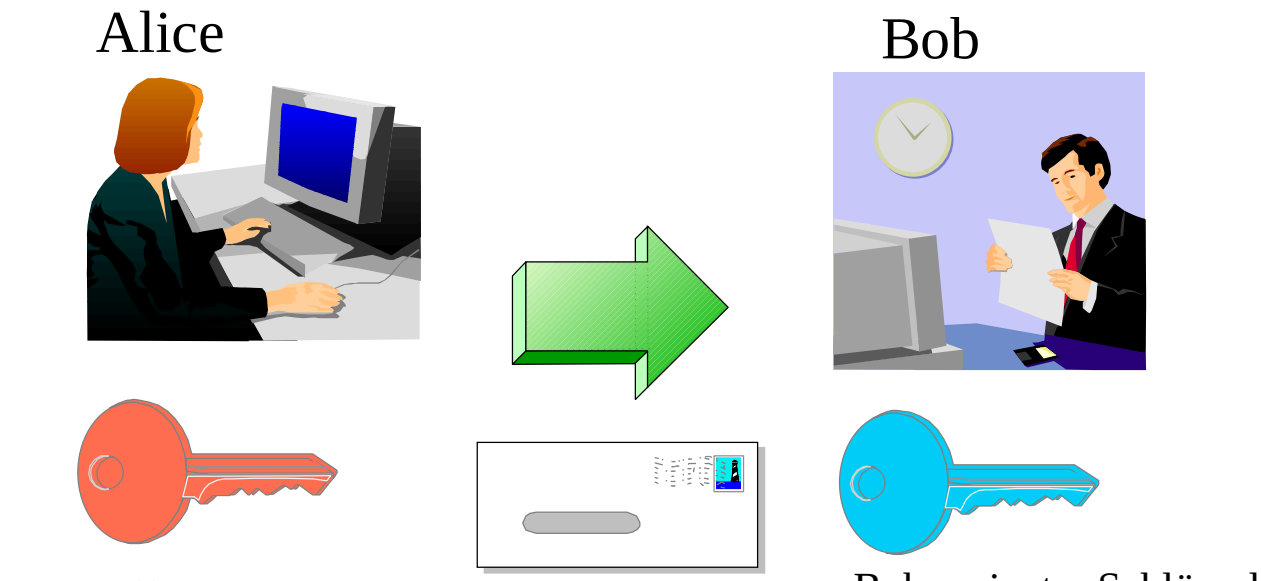


Alice verschlüsselt eine Nachricht mit dem geheimen Schlüssel und schickt sie an Bob. Bob entschlüsselt die Nachricht mit dem selben geheimen Schlüssel.

Public Key Kryptographie (asymmetrisch)

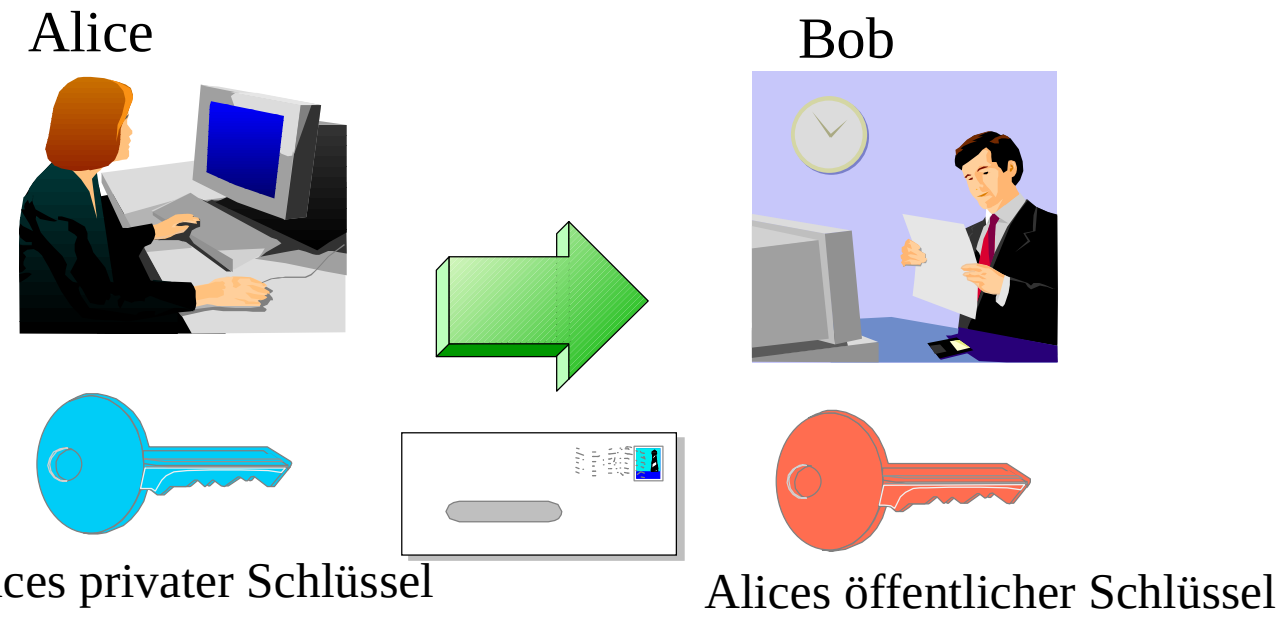
- **Es gibt eine „öffentlichen Schlüssel“ und eine "privaten Schlüssel"**
- **Der „private Schlüssel“ muss geheim gehalten werden**
- **Der „öffentliche Schlüssel" kann veröffentlicht werden**
- **Asymmetrische Kryptographie basiert auf mathematischen Problemen, die viel einfacher zu erzeugen sind, als man sie lösen kann (sehr große Primzahlen)**
  - RSA Rivest Shamir Adleman
  - DSA Digital Signature Algorithm
- **Typische Schlüssellängen: 512, 1024 oder 2048 Bit**

Public Key Kryptographie - Verschlüsseln



Alice verschlüsselt eine Nachricht mit Bobs öffentlichen Schlüssel und schickt sie an Bob. Bob entschlüsselt die Nachricht mit seinem privaten Schlüssel. Da nur er seinen privaten Schlüssel kennt, kann nur er Nachricht lesen.

Public Key Kryptographie - Signieren



Alice verschlüsselt die Nachricht mit ihrem privaten Schlüssel und schickt sie an Bob. Bob entschlüsselt sie mit Alices öffentlichen Schlüssel. Die Nachricht wurde von Alice "signiert" da sie nur mit **ihrem** öffentlichen Schlüssel entschlüsselt werden kann.

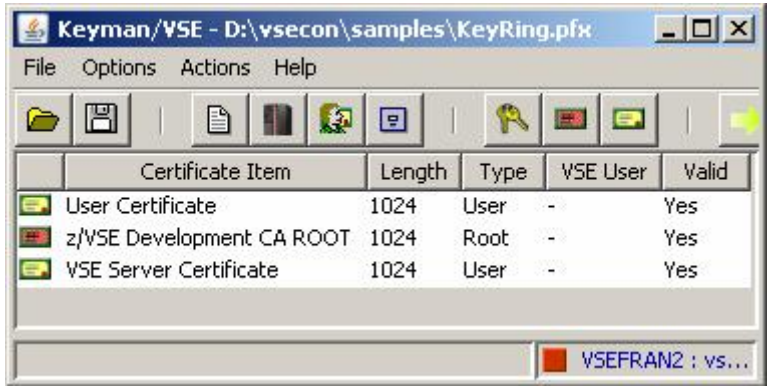
Zertifikate

- **Ein Zertifikat enthält die folgenden Informationen**
  - Das so genannte Subject (Name der Person)
  - Der öffentliche Schlüssel vom Subject
  - Gültigkeitsdauer
  - Name des Ausstellers (Issuer)
  - Eine Signatur des Ausstellers

- **Der Aussteller "signiert" das Zertifikat indem er einen Hash von dem Zertifikat mit seinem privaten Schlüssel verschlüsselt**
- **Die Signatur kann von jedem geprüft werden, indem man den Hash mit der öffentlichen Schlüssel des Ausstellers entschlüsselt und mit einem selbst erzeugten Hash vergleicht.**

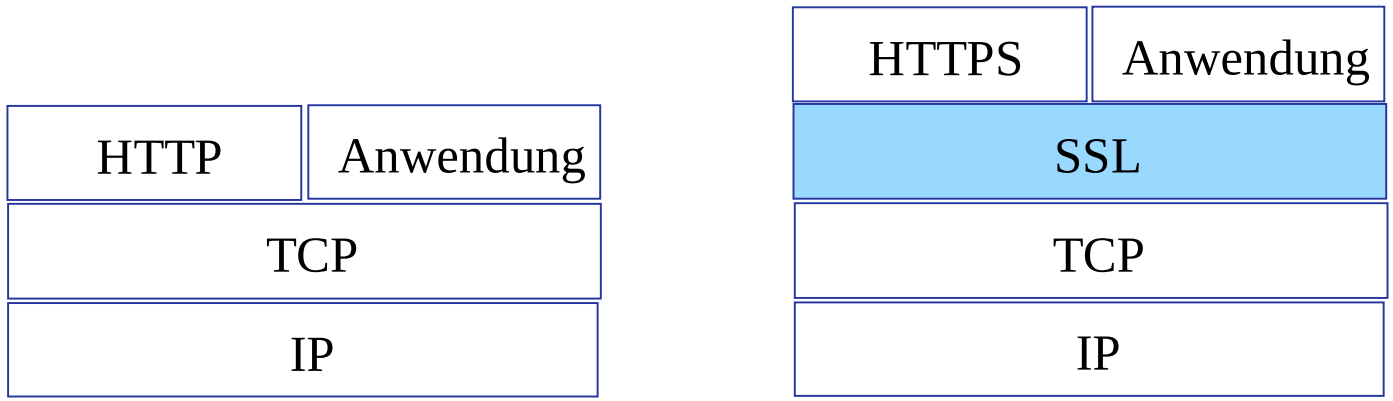
Schlüssel Management

- **Schlüssel Management ist nicht trivial**
  - Schlüssel müssen oft über viele Jahre aufgehoben werden
  - Schlüssel müssen den verschlüsselten Daten zugeordnet werden können
  - Verschlüsselte Daten und Schlüssel sind strikt zu trennen
- **Keyman/VSE**
  - Erzeugen und verwalten von RSA Schlüsseln und Zertifikaten
  - Hochladen von RSA Schlüsseln und Zertifikaten ins VSE
  - Erzeugen von PKCS#12 Keyring Dateien (für Java-based connector oder zum Import in einen Web Browser)
  - Download von der VSE Homepage http://www.ibm.com/servers/eserver/zseries/zvse/downloads/#vkeyman



SSL (Secure Socket Layer)

- **Wie der Name schon sagt, ist SSL ein Layer oberhalb von TCP**
- **SSL verwendet eine TCP Verbindung um die Daten verschlüsselt zu übertragen**
  - Asymmetrische Verschlüsselung für den Session Aufbau
  - Symmetrische Verschlüsselung für den Daten Transfer
- **Beispiele: HTTPS, VPN, Bankverbindungen, SecrureFTP, Secure tn3270**
- **IBM Middleware setzt auf sichere Verbindungen (MQ, CTG, VSE Connectors, …)**



Hardware Crypto mit VSE

VSE Release	Hardware Crypto
z/VSE 4.1	Ja (PCICA, CEX2C, CEX2A, CPACF)
z/VSE 3.1	Ja (PCICA, CEX2C, CEX2A, CPACF)
VSE/ESA 2.7	Ja (PCICA)
VSE/ESA 2.6	Nein

Crypto Card	z800	z900	z890	z990	z9 BC, z9 EC
PCICA	Ja	Ja	Ja	Ja	Nein
CEX2C	Nein	Nein	Ja	Ja	Ja
CPACF	Nein	Nein	Ja	Ja	Ja
CEX2A	Nein	Nein	Nein	Nein	Ja

Hardware Crypto mit VSE

- **Keine spezielle Hardware Konfiguration nötig im VSE**
  - Keine IOCDS Definitionen
  - Kein spezieller Device Type
  - Kein ADD Statement in der IPL Procedure
  - Unter Umständen Definition im LPAR oder z/VM

- **Crypto Devices werden beim IPL automatisch erkannt**
  - HW Crypto wird automatisch verwendet wenn vorhanden
    - z.B. SSL oder CryptoVSE API
  - Keine Änderungen in Crypto-Anwendungen nötig

```
FB 0095 1J023I FOUND A CRYPTO EXPRESS2 CARD AT DEVICE INDEX 0
FB 0095 1J023I FOUND A CRYPTO EXPRESS2 CARD AT DEVICE INDEX 1
FB 0095 1J014I FOUND A PCICA CARD AT DEVICE INDEX 6
FB 0095 1J014I FOUND A PCICA CARD AT DEVICE INDEX 7
FB 0095 1J005I HARDWARE CRYPTO ENVIRONMENT INITIALIZED SUCCESSFULLY.
FB 0095 1J006I USING CRYPTO DOMAIN 0
FB 0095 1J022I CPU CRYPTOGRAPHIC ASSIST FEATURE AVAILABLE.
```

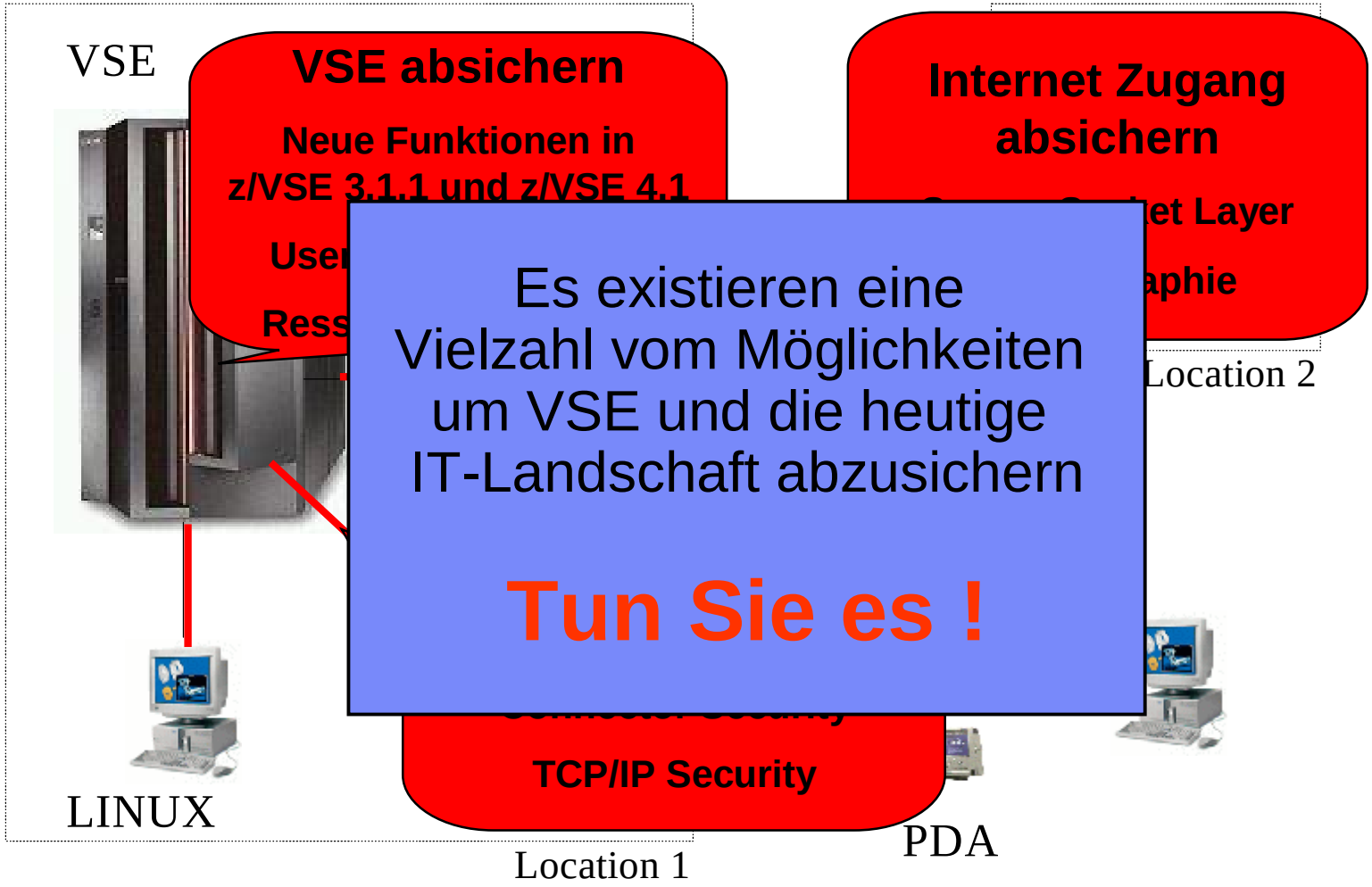
IBM Tape Encryption – TS1120

- **Das IBM System Storage TS1120 Tape Drive unterstützt das Verschlüsseln der Daten im Tape Drive selbst**
  - Separater IBM Encryption Key Manager
    - Läuft auf einer Java Plattform (z.B. Linux, Unix, Windows)
    - Verwaltet und erstellt die Schlüssel
    - Kommuniziert mit dem Tape Drive
- **Im z/VSE 4.1 Anouncement:**
  - *„z/VSE V4.1 is designed to exploit Systems Managed Encryption with the IBM System Storage TS1120“*
  - *“This function will not be available at z/VSE V4.1 general availability. The function is planned to be delivered later via PTF. If you plan to use this function, check the z/VSE Web site after GA for the latest status.”*
  - Die Unterstützung wird per PTF nachgeliefert (auch für z/VSE 3.1)

Möglichkeiten zum Verschlüsseln von Backups

- **IBM System Storage TS1120 Tape Drive**
- **Mit VSE Virtual Tape (VTAPE)**
  - Backup per VTAPE auf Remote-System
  - Das Tape Image kann auf einem verschlüsselten Medium gespeichert werden
    - Verschlüsselte Datei Systeme oder Verzeichnisse (z.B. EcryptFS unter Linux)
    - Verschlüsselungs-Tools (z.B. TrueCrypt)
    - Tivoli Storage Manager (z.B. auf Linux)
- **Verschlüsseln der Daten in den Anwendungen**
  - CryptoVSE API bietet alle benötigten Crypto-Funktionen
    - Verwendet Hardware Crypto Support wenn verfügbar

IT Sicherheit in einem heterogenen Umfeld



Fragen ?